UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PHILLIP TORETTO and DANIEL C. KING, individually and on behalf of all others similarly situated, Plaintiffs, v. DONNELLEY FINANCIAL SOLUTIONS, INC. and MEDIANT COMMUNICATIONS, INC., Defendants.	Case No. 1:20-cv-2667

CLASS ACTION COMPLAINT

Plaintiffs Phillip Toretto and Daniel King, individually and on behalf of all persons similarly situated, bring this Class Action Complaint against Donnelley Financial Solutions, Inc. ("Donnelley") and Mediant Communications, Inc. ("Mediant") (collectively, "Defendants"), based upon personal knowledge with respect to themselves, through limited discovery during litigation regarding the same dispute against Mediant in the Northern District of California, and review of public documents as to all other matters.

INTRODUCTION

1. Public companies and mutual funds hire Donnelley as their proxy agent to distribute materials to shareholders, coordinate shareholder votes, and tabulate voting results. Donnelley holds Mediant out as its "partner" responsible for carrying-out its clients' proxy services, claiming the companies "offer the industry's only single-source solution for start-to-finish fund proxy

services."[1] To obtain Donnelley's and Mediant's "single-source solution" for proxy services, companies entrust Donnelley with sensitive shareholder information in order to effectuate the distribution of materials and the coordination of important votes. Donnelley, in turn, shares that sensitive shareholder information with Mediant. In some instances, companies contract with Mediant directly for its proxy services.

2. On April 1, 2019, hackers obtained unauthorized access to four of Mediant's business email accounts and exfiltrated the personal information of its customers' investors (the "Data Breach"). The stolen information included a host of sensitive personal and financial information, including investors' names, genders, physical addresses, email addresses, phone numbers, Social Security Numbers, tax identification numbers, and bank account numbers, as well as specific information relating to investors' securities holdings, including securities units purchased, dates of purchase, and individuals or entities designated to collect investment payments (hereafter, collectively referred to as "Personal Information").

3. Mediant—a company that touts itself as employing cutting-edge technology—is responsible for allowing the breach to occur by failing to implement and maintain reasonable safeguards and failing to comply with industry-standard data security practices, contrary to the representations made in Mediant's privacy policy.

4. Likewise, Donnelley—a company that claims to be "revolutionizing regulatory and financial technology"[2]—is responsible for the Data Breach by partnering with Mediant, and

[1] *See* The Perfect Partnership to Power Your Fund Proxies, https://www.dfinsolutions.com/insights/fact-sheet/dfin-and-mediant-perfect-partnership-power-your-fund-proxies (last visited March 23, 2020).

[2] Donnelley, *About*, https://www.dfinsolutions.com/about (last visited March 23, 2020).

transferring Plaintiffs' and Class Members' most sensitive Personal Information to it, when Donnelley knew or should have known Mediant was unequipped to protect it.

5. As a result of Defendants' failure to protect the information in their possession, Plaintiffs and Class Members have suffered or are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Moreover, although Mediant discovered the breach the same day that it occurred, it waited almost two months to notify impacted shareholders, thereby knowingly exposing vulnerable individuals to further harm.

PARTIES

6. Plaintiff Phillip Toretto is a resident and citizen of Sausalito, California, whose Personal Information was compromised in the Data Breach.

7. Plaintiff Daniel C. King is a resident and citizen of Wharton, New Jersey, whose Personal Information was compromised in the Data Breach.

8. Donnelley is a global risk and compliance solutions company headquartered in Chicago, Illinois, and incorporated under the laws of the State of Delaware.

9. Mediant is an investor communications and financial technology company headquartered in New York, New York, and incorporated under the laws of the State of Delaware.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332, the Class Action Fairness Act, because: (i) there are 100 or more class members; (ii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; and (iii) there is minimal diversity because at least one plaintiff and one defendant are citizens of different states.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving risk to the claim occurred here, and § 1391(c)(2)

because Defendants are subject to this Court's personal jurisdiction in this action. Among other things, Mediant maintains its corporate headquarters in this District, Defendants conduct business in this District, and Defendants purposefully availed themselves to this District, directed their activities to this District, and consummated numerous transactions in this District.

STATEMENT OF FACTS

A. The Data Breach

12. Donnelley holds itself out as "a leader in risk and compliance solutions, providing insightful technology, industry expertise and data insights to clients across the globe."[3] Claiming to "deliver confidence with the right solutions in moments that matter,"[4] Donnelley offers an array of products and services in technology, fintech, financial solutions, IPO, M&A, proxy, global filings, GDPR, ESG, capital markets, investment markets, e-delivery, blockchain, and data management.[5]

13. Mediant holds itself out as a leader in investor communications, offering "game-changing new technologies for banks, brokers, fund companies, and issuers." [6] In its marketing materials, Mediant summarizes its offerings as follows:

[3] Donnelley, *About*, https://www.dfinsolutions.com/about (last visited March 23, 2020).

[4] Donnelley, *Linkedin About Us*, https://www.linkedin.com/company/dfinsolutions (last visited March 23, 2020).

[5] *Id.*

[6] Mediant 2018 Proxy Guide, Corporate Issuer Services, https://www.proxydocs.com/branding/212121/2018/files/assets/common/downloads/Mediant%202018%20Annual%20Proxy%20Guide%20.pdf (last visited March 23, 2020).

WHAT WE DO

Mediant offers a wide range of solutions for the investor communications lifecycle, all via our single, integrated MIC platform. Whether you're a financial advisor or a back-office professional, our centralized platform gives you access to the real-time, actionable information you need.

MEDIANT PROVIDES A COMPREHENSIVE SUITE OF SOLUTIONS FOR:

PROXY
- Highly scalable print, electronic, and mail management
- Extensive data analytics, robust tabulation, and reporting
- End-to-end proxy meeting support

CORPORATE ACTIONS
- Custom-branded print and electronic corporate action communications
- Electronic corporate action documents and source materials stored online

REGULATORY REPORT DISTRIBUTION
- Robust in-house fulfillment for control over entire regulatory report distribution process
- Automated process and better insight and tracking

STATEMENTS & TRADE CONFIRMS
- Flexible, scalable management of statement and trade confirms
- Secure and on-time distribution and delivery

ANYTIME, ANYWHERE ACCESS
- Quick and easy electronic access to all of our solutions from any device

FULFILLMENT SERVICES
- Technology-enabled print, mail, and fulfillment services
- Secure facility successfully processes and distributes millions of investor communications documents each year

REGULATORY COMPLIANCE SERVICE
- Comprehensive business rules surrounding applicable regulatory requirements
- Regulatory updates and support from compliance specialists

TURN-KEY E-DELIVER & ARCHIVING
- SEC-compliant electronic delivery and document archive solution
- Streamlined e-consent process with custom, user-friendly sites

PROSPECTUS SERVICES
- Comprehensive in-house print and mail system for timely and efficient prospectus delivery
- Complete and compliant support for T+1 prospectus fulfillment, pre-sale delivery, combined confirms

14. Donnelley, with Mediant, claims to provide "the perfect partnership to power [their clients'] fund proxies," touting the pair as "the industry's only single-source solution for start-to-finish fund proxy services."[7]

[7] *See* The Perfect Partnership to Power Your Fund Proxies, https://www.dfinsolutions.com/insights/fact-sheet/dfin-and-mediant-perfect-partnership-power-your-fund-proxies (last visited March 23, 2020).

15. On April 1, 2019, hackers obtained unauthorized access to Mediant's business email accounts and exfiltrated the Personal Information of its and Donnelley's customers' investors. According to Mediant, it discovered the unauthorized access that same day and disconnected the affected server from the company's system. Mediant then commenced an investigation into the breach, but did not take any action at the time to notify either its impacted customers or their investors.

16. At the end of May 2019, almost two full months after Mediant discovered the Data Breach, Mediant began notifying state attorneys general and sending notices to its customers' investors whose Personal Information had been stolen. Mediant sent notice to over 200,000 individuals in all fifty states and the District of Columbia and Puerto Rico. The affected individuals were investors in 15 entities and mutual funds located in California, Illinois, Kansas, Massachusetts, Michigan, Missouri, and New York. Mediant learned which entities and mutual funds had affected investors from Donnelley, who had the direct contractual relationship with most of the affected entities and mutual funds.

17. In responding to inquiries from state regulators in the aftermath of the Data Breach, Mediant disclosed that the Data Breach was the result of a criminal hack wherein hackers obtained unauthorized access to four Mediant business email accounts exploiting a vulnerability in Mediant's email system that allowed the hacker to gain access to Personal Information located on a network server. Following the Data Breach, Mediant stated that it had taken steps to strengthen the security of its systems—such as remediating the vulnerability in its email system, implementing targeted network access restrictions, updating network monitoring systems, requiring affected employees to change their passwords, and accelerating planned improvements to its email system. Mediant also stated it would also be reviewing its written information security program to

determine if any updates to the program were appropriate. It further admitted that it had not encrypted the Personal Information stored in its systems.

18. According to the sample notices provided to state attorneys general, Mediant's notification letters contain a list of the company or companies from which the affected investors' information was stolen and a list of the specific types of Personal Information stolen from the investor during the Data Breach. For example, according to the specific notice for Jackson National Life Insurance Company posted on the California State Attorney General's website, the stolen investor information from that company included investors' full names, genders, physical addresses, email addresses, phone numbers, Social Security Numbers, tax identification numbers, account numbers, and various other specific types of information such as units owned, issue dates, and owner/annuitant designation.[8]

19. Sample notices posted to the websites of the Vermont and California Attorneys General explained that Mediant "provides many mutual funds and public companies, including real estate investment trusts, with mailing and document processing services as well as services in connection with their annual and special shareholder meetings, including the distribution of proxy materials, coordination of votes, and tabulation of voting results. Mutual funds and public companies hire proxy agents such as Mediant in connection with their shareholder meetings as a

[8] State of California Department of Justice, *Jackson National Life Insurance Company Notice*, https://oag.ca.gov/system/files/CA%20Consumer%20Notice_Mediant_Sample_0.pdf# (last visited March 23, 2020).

matter of standard practice."[9] Mediant disclosed that it received the shareholders' information "while providing its services to entities related to [the affected person's] ownership of certain securities."

20. The notices provided that on May 10, 2019, Mediant had "determined [the recipient shareholder's] personal information was among the information impacted." Yet, instead of immediately notifying affected individuals, Mediant "first informed" the companies whose shareholders were impacted—two weeks prior to notifying the shareholders themselves.

21. Mediant represented that none of the companies who provided investor information had systems involved in the incident or "were otherwise at fault in the incident."

22. All of the sample notices represented that Mediant has "taken steps to strengthen [its] protection of personal information, including updating our network security controls and email systems."[10] Mediant provided no explanation as to why its network security controls and email systems were not sufficiently updated and their vulnerabilities remedied prior to a malicious and unauthorized party gaining access to extremely sensitive Personal Information of its and Donnelley's customers' investors. The criminal hackers would not have been able to gain access to four email accounts simultaneously but for Mediant maintaining deficient controls to prevent and monitor for unauthorized access.

---

[9] *See, e.g.*, Office of the Vermont Attorney General, *Notice of Data Breach*, https://ago.vermont.gov/blog/2019/05/31/mediant-communications-sbn-to-consumers/ (last visited March 23, 2020); *see also* State of California Department of Justice, *Submitted Breach Notification Sample*, https://www.oag.ca.gov/system/files/L01_Mediant_%20General_0.pdf (last visited March 23, 2020); State of California Department of Justice, Jackson National Life Insurance Company Notice, https://oag.ca.gov/system/files/CA%20Consumer%20Notice_Mediant_Sample_0.pdf# (last visited March 23, 2020).

[10] *See* State of California Department of Justice, *Submitted Breach Notification Sample*, https://www.oag.ca.gov/system/files/L01_Mediant_%20General_0.pdf (last visited March 23, 2020).

23. Mediant further stated that it will "continue to closely monitor and take further steps to safeguard such information"; had "reported the matter to law enforcement, but this notice has not been delayed because of law enforcement investigation"; and is "offering credit monitoring for a period of 24 months at no cost to [the impacted investors]." Mediant recommended that the affected investors take steps themselves to prevent fraud and identity theft, telling them to "closely review or monitor [their] financial accounts, statements, credit reports and other financial information for any evidence of unusual activity, fraudulent charges or signs of identity theft." The notice attaches three pages containing "additional information" regarding steps the affected investors can take, including implementing security freezes and fraud alerts and providing the contact information for certain state attorneys general who can provide additional information about "steps [the affected investors] can take to prevent identity theft."

24. Mediant's recommendation reflects the imminent risk affected investors now face where sophisticated criminal hackers stole and now possess Personal Information with the clear intent to misuse it. Indeed, the targeted nature of the hack, coupled with the exfiltration of individuals' most highly-sensitive personal and financial information, strongly suggests the purpose of the hacks was for illicit financial gain by trading on investors' Personal Information.

25. Unfortunately, Mediant's notification to affected individuals was severely deficient in that it: (1) failed to disclose precisely how Mediant obtained affected individuals' information; (2) failed to disclose precisely how the Data Breach occurred, including the method by which its email accounts were accessed or the information exfiltrated; (3) failed to disclose how many people were affected; (4) failed to disclose who was responsible for the Data Breach and how many unauthorized individuals had access to the stolen information; and (5) failed to disclose the results of any investigations into the Data Breach. Likewise, though Donnelley was responsible in most

instances for transferring the Personal Information to Mediant, it made no effort to notify affected individuals itself or remedy any of the deficiencies in Mediant's notification.

26. By keeping affected individuals in the dark about the key details surrounding the Data Breach, Donnelley and Mediant have prevented affected individuals from taking meaningful, proactive, and targeted mitigation measures that could help protect them against severe harm.

27. Had Defendants provided timely and adequate notice of the Data Breach, Plaintiffs and Class Members could have taken appropriate measures sooner to avoid some of the harms they have suffered, including avoiding unauthorized charges, cancelling or changing usernames and passwords on compromised accounts, monitoring their account information and credit reports for fraudulent activity, including purchasing credit monitoring services sooner, and contacting their banks to alert them of the risk of fraud.

B. Plaintiff Toretto's Allegations

28. Following the Data Breach, Plaintiff Toretto received a letter from Mediant dated May 31, 2019, stating that his Personal Information had been compromised during the Data Breach.

29. Specifically, the letter stated that "Mediant received your personal information while providing its services to entities related to your ownership of certain securities including: Blackstone Real Estate Income Trust, Inc. (2017 annual meeting)." The letter disclosed that Plaintiff Toretto had the following information compromised: "your name, address, email address, phone number, Social Security Number/tax identification numbers, and transfer agent's account ID."

30. The letter advised Plaintiff Toretto to "be vigilant and closely review or monitor your financial accounts, statements, credit reports and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft."

31. As a result of the Data Breach, Plaintiff Torretto has expended time and effort regularly monitoring his financial and credit accounts in order to mitigate against potential harm. In the wake of the Data Breach, Plaintiff Torretto spent many hours checking his accounts to mitigate against potential harm. He also now regularly expends time and effort due to the Data Breach checking his accounts routinely for unauthorized activity and checking his credit reports monthly to ensure that no unauthorized accounts have been opened in his name.

32. To help protect himself following the Data Breach, Plaintiff Torretto purchased a LifeLock service plan which after the first year will result in an annual out-of-pocket fee of $300. In addition, Plaintiff Torretto has obtained Kaspersky security plans for each of his computers at an annual cost of approximately $100.

33. Plaintiff Torretto also began to receive a significant increase in spam-related telephone calls following the Data Breach, which interfered with work, travel and daily life. Plaintiff Torretto has had to pay out-of-pocket for Verizon's Call Filter and Digital Secure services at a cost of approximately $17 per month to help protect against these calls.

34. Given the highly-sensitive nature of the information stolen, Plaintiff Toretto remains at a substantial and imminent risk of future harm. He is also harmed because his Personal Information is less valuable to him as a personal-identifier now that criminals can use it to impersonate him to fraudulent ends.

C. Plaintiff King's Allegations

35. Following the Data Breach, Plaintiff King received a letter from Mediant dated May 31, 2019, stating that his Personal Information had been compromised during the Data Breach.

36. Specifically, the letter stated that "Mediant received your personal information while providing its services to entities related to your ownership of certain securities including: Ivy

Natural Resources Fund's 2019 proxy." The letter disclosed that Plaintiff King had the following information compromised: "your name, address, Social Security Number/tax ID number, and transfer agent's account ID."

37. The letter advised Plaintiff King to "be vigilant and closely review or monitor your financial accounts, statements, credit reports and other financial information for any evidence of unusual actively, fraudulent charges, or signs of identity theft."

38. As a result of the Data Breach, Plaintiff King has expended time and effort regularly monitoring his financial and credit accounts in order to mitigate against potential harm. In the wake of the Data Breach, Plaintiff King spent several hours checking his accounts to mitigate against potential harm. He also now regularly expends time and effort due to the Data Breach by checking his accounts daily to ensure there have been no unauthorized charges and checking his credit reports monthly to ensure that no unauthorized accounts have been opened in his name.

39. Further, after the Data Breach, Plaintiff King twice experienced fraudulent charges on a retail credit card. In June of 2019, he experienced $1,750 in fraudulent charges on the card, which was ultimately reimbursed after time and effort expended by Plaintiff King. Then, in August 2019, he experienced $2,700 in unauthorized charges on the same card, which was also reimbursed. While investigating the fraud, Plaintiff King was informed by the retail credit card that it seemed likely the fraud had been perpetrated by an individual who did not have access to the card number but rather had access to his personal information which was used to look up and use the retail credit card at the stores and impersonate him.

40. Given the highly-sensitive nature of the information stolen, Plaintiff King remains at a substantial and imminent risk of future harm. He is also harmed because his Personal

Information is less valuable to him as a personal-identifier now that criminals can use it to impersonate him to fraudulent ends.

D. Defendants Knew They were a Target of Cyber-Threats

41. Donnelley touts its "insightful technology" in providing its risk and compliance solutions to clients across the globe.[11] Likewise, Mediant touts its "leading technology and strict compliance with industry regulations, which allows clients to balance innovation with requirements."[12]

42. On its website, Mediant touts its "web-based technology" and "industry-leading security." Mediant represents that it maintains a "Comprehensive cybersecurity program with highly robust, redundant infrastructure platform that provides reliability and security you need."[13] It further states that, "We undergo annual audits and comply with all federal, state, and industry privacy and security regulations."[14]

43. In Donnelley's Privacy Notice published on its website and available to all of its customers' investors, Donnelley states it "respect[s] your privacy and know[s] that you care about how [it] use[s] and share[s] your information."[15] The notice states that Donnelley collects a variety of basic and sensitive personal information through its website and interactions with users, as well

[11] Donnelley, *About*, https://www.dfinsolutions.com/about (last visited March 23, 2020).

[12] Mediant, *Company Profile*, https://mediantinc.com/about/ (last visited March 23, 2020).

[13] Mediant, *Technology*, https://www.mediantinc.com/why-mediant/technology (last visited March 23, 2020).

[14] *Id*.

[15] Donnelley, *Privacy Notice*, https://www.dfinsolutions.com/privacy-notice?_ga=2.122645259.1080842663.1584104880-1327891255.1583944656 (last visited March 23, 2020).

as from third parties, including Donnelley's business partners, contractors, analytics and other service providers."[16]

44. Donnelley's Privacy Notice states "the security of your personal information is important to us," and promises to "use reasonable physical, electronic and procedural safeguards to protect the personal information we collect," including "us[ing] reasonable measures to safeguard personally identifiable information from loss, theft, misuse, alteration and unauthorized access or destruction. In addition, we maintain appropriate physical, electronic, and procedural safeguards to protect your personal data."[17] Donnelley also promises that it "regularly reviews [its] compliance with [its] Privacy Notice," and "adhere[s] to several self-regulatory frameworks in addition to complying with applicable laws."[18]

45. Likewise, in Mediant's Privacy Policy published on its website and available to all of its customers' investors, Mediant states that it is committed to maintaining the privacy of shareholders' Personal Information, which Mediant defines to include names, account numbers, physical addresses, e-mail addresses, the number of shares that you own, and other information that can be used to identify the person. Mediant promises that personally identifiable data "provided to Mediant by you or by third parties will be kept confidential."[19]

46. Further, Mediant represents that it "maintains physical, electronic and procedural safeguards in accordance with laws and regulations governing confidentiality and security of information. Access to personal information is limited to only those workers and third parties who need access to the information to perform necessary activities for Mediant. We also provide security

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] Mediant, *Privacy Policy*, https://mediantinc.com/privacy-policy (last visited March 23, 2020).

for your information by maintaining servers that are secure and dedicated solely to the services that we provide to protect against loss, misuse, or alteration of your information."[20]

47. As financial technology firms that tout their "game-changing"[21] and "insightful"[22] technologies, Defendants are fully aware of the dangers data breaches pose to companies who compile investor information.

48. In fact, Donnelley's Chief Information Security Officer (CISO), Dannie Combs, stated in an interview published on Donnelley's website that the company "house[s] millions of records that are uniquely valuable," and recognized that a data breach would be deleterious to its and its clients' businesses. He also recognized that "privacy is now the law in most of the world," and acknowledged that Donnelley is "certainly on the front lines of the cyber warfare battlefield each and every day." He stated that "it takes everyone in the entire company to be secure. Whether it is those who are writing code and are cognizant of security use cases, those in client services who are handling our clients' information or those in HR, the whole company must be intensely focused on security."[23] Despite these proclamations, Donnelley purportedly did not require its "partners" like Mediant to execute a written contract requiring them to implement reasonable data security measures and granting Donnelley audit rights to ensure such measures are being followed.[24]

---

[20] *Id.*

[21] Mediant, *MIC Platform*, https://mediantinc.com/solutions/mic-platform (last visited March 23, 2020).

[22] Donnelley, *About*, https://www.dfinsolutions.com/about (last visited March 23, 2020).

[23] Same Battle, Different Field: A Conversation With Our Chief Information Security Officer, https://www.dfinsolutions.com/insights/article/same-battle-different-field-conversation-our-chief-information-security-officer (last visited March 23, 2020).

[24] Following the Data Breach, an attorney for Mediant represented that Mediant and Donnelley never had a written contract governing their partnership or the exchange of personal information between the parties as it relates to the entities impacted by this breach.

49. Similarly, Mediant's Chief Technology Officer (CTO), Stacey Robinson, wrote an article in 2017 specifically addressing the severe threat cyber-attacks pose to the financial industry and companies like Mediant. The article, entitled "Cyber Attacks May Make Financial Industry 'WannaCry,"[25] is posted on Mediant's website and was published at WealthManagement.com.

50. In the article, Mediant's CTO recognized that "[l]arge-scale cybersecurity breaches are in the news on a weekly and even daily basis" and that the "financial services industry is a huge target for cybercriminals — more than any other industry — and the risk has evolved from financial theft and fraud to more complex and serious consequences like theft of intellectual property, business disruption and reputation damage (Deloitte). In other words, hackers are not just stealing lists of Social Security numbers anymore, but rather executing serious breaches with more far-reaching consequences."[26]

51. Mediant's CTO explained that "at financial services firms, cyberattacks exploit flaws in security programs that allow threat actors to gain access. Among the most common attack targets are endpoints, such as laptops, tablets and smartphones. Endpoints are particularly vulnerable because they require both robust security protocols and effective education for the firms' employees, who act as the last line of defense. Attackers use weaponized email attachments and links to attack sites in order to compromise credentials and establish a foothold on the endpoint. The 2016 Data Breach Investigations Report (DBIR) from Verizon points out that it only takes minutes to compromise a host and collect a set of valid credentials, and in most cases, data exfiltration is underway just days after compromise."[27]

---

[25] Robinson, Stacey, Cyber Attacks May Make Financial Industry "WannaCry," Wealth Management (May 24, 2017), https://www.wealthmanagement.com/technology/cyber-attacks-may-make-financial-industry-wannacry.

[26] *Id.*

[27] *Id.*

52. Mediant's CTO described why "endpoints," such as email accounts are especially vulnerable: "Compromising an endpoint gives the attacker a lot of bang for their buck, since they provide easy access to additional data and systems. One of the most effective ways to exploit endpoint security vulnerability is via phishing, a form of social engineering that commonly targets financial services companies. Per the DBIR, 30 percent of phishing emails were opened and 12 percent clicked on the malicious attachment or link, thereby enabling the attack."[28]

53. Mediant's CTO also acknowledged that cyber-attacks can be prevented: "Successful endpoint security is a complex endeavor, requiring an extensive framework and consistent attention. It requires quality and maturity in areas such as OS hardening, the principle of least privilege and patching. Particular consideration should be paid to advanced security solutions around application whitelisting, exploit detection and prevention, device blocking, firewalls, web filtering and malware prevention. While attackers will continue to use phishing as an attack vector in order to capitalize on human error, it's certainly possible — and these days, essential — to develop and implement a robust security framework that accounts for all vulnerabilities."[29]

54. As acknowledged by Defendants' chief information security officers and reflected in their privacy statements, Defendants were at all times fully aware of their obligation to protect investors' Personal Information and the risks associated with failing to do so. Indeed, Defendants observed frequent public announcements of data breaches affecting financial industries and knew that information of the type collected, maintained, and stored by Defendants is highly coveted and a frequent target of hackers.

[28] *Id.*

[29] *Id.*

55. Indeed, a February 2018 report prepared by the Identity Theft Resource Center (ITRC) noted that, "For years, the financial services sector globally has been a primary target for attacks by cybercriminals largely because of the tremendous value of the information available. In fact, financial services firms are reportedly hit by security incidents a staggering 300 times more frequently than businesses in other industries. This startling statistic underscores the importance of financial services professionals being aware of the breadth and causes of successful cyberattacks and also their need to keep their knowledge of risk mitigation strategies current."[30]

56. In its 2019 Data Breach Investigations Report, Verizon noted that there were 927 breaches affecting the insurance and financial industries in 2018 alone, with confirmed data disclosure in 207 of the breaches.[31] The report found that 71% of breaches are "financially motivated" meaning the hackers accessed information with the intention to profit from it.

57. Defendants also observed numerous other well-publicized data breaches involving major corporations that were targeted for the sensitive consumer information they retained. For example, in early 2015, Anthem, Inc., the second-largest health insurer in the United States, suffered a massive data breach exposing the names, addresses, Social Security numbers, dates of birth, and employment histories of nearly 80 million current and former plan members nationwide.[32]

---

[30] ITRC, *The Impact of Cybersecurity Incidents on Financial Institutions* (Feb. 2018), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf (last visited March 23, 2020).

[31] Verizon, *2019 Data Breach Investigations Report*, available with subscription at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

[32] C. Riley, *Insurance Giant Anthem Hit by Massive Data Breach*, CNN (Feb. 6, 2015), https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/ (last visited March 23, 2020).

58. In March 2015, health insurer Premera Blue Cross announced it suffered a data breach that exposed the medical data and financial information of 11 million customers, including claims data, clinical information, banking account numbers, Social Security numbers, birth dates and other data in an attack that began in May 2014.[33] Shortly thereafter, New York-based insurer Excellus BlueCross BlueShield announced a breach that exposed the personal information of 10 million of its plan members in an attack dating back to 2013.[34]

59. Through a series of data breaches extending back to 2013, more than three billion Yahoo! user accounts were compromised when users' names, addresses, and dates of birth were stolen.[35]

60. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target and the Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.[36]

61. In September 2017, credit reporting agency Equifax announced that hackers stole the personal and financial information of 147 million Americans between May and July 2017.[37]

---

[33] *Premera Blue Cross Says Data Breach Exposed Medical Data*, THE NEW YORK TIMES (March 1, 2015), https://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html (last visited March 23, 2020).

[34] *Cyber Breach Hits 10 Million Excellus Healthcare Customers*, USA TODAY (Sept. 10, 2015), https://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/ (last visited March 23, 2020).

[35] S. Larson, *Every Single Yahoo Account was Hacked – 3 Billion in All*, CNN (OCT. 4, 2017), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html (last visited March 23, 2020).

[36] B. Krebs, *Home Depot Hit By Same Malware as Target*, KREBS ON SECURITY (Sept. 14, 2014), https://krebsonsecurity.com/tag/home-depot-databreach/ (last visited March 23, 2020).

[37] Equifax 2017 Cybersecurity Incident & Important Consumer Information, https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited March 23, 2020).

The following year, hotel giant Marriott announced that 383 million guest records were exfiltrated from its hotel guest reservation database over a four-year period.[38]

62. Despite its retention of highly-sensitive information, Mediant failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its databases. Likewise, while claiming to use leading security practices to protect Personal Information while it resided on its own systems, Donnelley did not use reasonable care to ensure that its partner had adequate data security to protect the Personal Information shared by Donnelley. Mediant had the resources to prevent a breach and made significant expenditures to promote its services, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting financial and other related industries. Donnelley should not have partnered with Mediant or shared sensitive Personal Information with it absent exercising adequate oversight to ensure such information was securely protected.

E. Defendants Failed to Comply with Regulatory Guidance

63. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[39]

[38] Marriott Provides Update on Starwood Database Security Incident, https://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/ (last visited March 23, 2020).

[39] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 23, 2020).

64. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[40] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[41]

65. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[42]

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C.

[40] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 23, 2020).

[41] *Id*.

[42] FTC, *Start With Security*, *supra* note 39.

§ 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[43]

67. In this case, Defendants were fully aware of their obligation to use reasonable measures to protect the personal information in their possession, acknowledging as much in their own privacy policies. Defendants also knew they were a target for hackers. But despite understanding the consequences of inadequate data security, Donnelley shared sensitive Personal Information with Mediant without exercising adequate oversight, and Mediant failed to comply with industry-standard data security requirements.

68. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

F. Donnelley Is Subject to the Gramm-Leach-Bliley Act

69. Donnelley is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

70. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

71. Donnelley collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Donnelley was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 *et seq*., and is subject to numerous rules and regulations promulgated under the GLBA statutes.

[43] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited March 23, 2020).

72. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of consumer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Donnelley violated the Safeguard Rule.

73. Donnelley's conduct resulted in a failure to follow GLBA mandated rules and regulations, many of which are also industry standard. In particular, the Data Breach demonstrates that Mediant failed to implement (or inadequately implemented) information security policies or procedures to protect the confidentiality of the Personal Information it maintained in its data systems. The Data Breach further demonstrates that Donnelley failed to oversee Mediant and to require Mediant to protect the security and confidentiality of its customers' investors' Personal Information.

74. Had Donnelley monitored Mediant and required it to have the necessary security measures in place to ensure it could protect the Personal Information in its possession, the Data

Breach could have been avoided and Plaintiffs' and Class Members' Personal Information would not have been stolen.

G. The Impact of the Data Breach on Affected Individuals

75. Given the highly-sensitive nature of the Personal Information stolen in the Data Breach, hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

76. In fact, many victims of the Data Breach have likely already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, and unauthorized access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

77. The Personal Information exposed in the Data Breach is highly-coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web"—exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial and investment accounts and records; (i) engage in mortgage fraud; or

(j) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

78. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[44] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

79. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.[45]

[44] Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited March 23, 2020).

[45] *Id.*

80. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[46]

81. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[47]

82. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the

[46] *Id.*

[47] FTC, *Combating Identity Theft A Strategic Plan* (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited March 23, 2020).

misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[48]

83. The unauthorized disclosure of the sensitive Personal Information to data thieves reduces its inherent value to its owner. As one court recently recognized: "Consumers recognize the value of their personal information and offer it in exchange for goods and services. To take a few examples, many business[es] offer goods and services such as wifi access, special access to products, or discounts in exchange for a customer's personal information. Consumer[s] choose whether to exchange their personal information for these goods and services every day. . . . [T]he value of personal identifying information is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their personal identifying information. . . . Similarly, the businesses that request (or require) consumers to share their personal identifying information as part of a commercial transaction do so with the expectation that its integrity as not been

[48] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), http://www.ssa.gov/pubs/10064.html (last visited March 23, 2020).

compromised." *In re Marriott International, Inc., Customer Data Sec. Breach Litig.*, No. 19-MD-2879, 2020 WL 869241, at *8 (D. Md. Feb. 21, 2020).

84. And consumers are injured every time their data is stolen and placed on the dark web—even if they have been victims of previous data breaches. Indeed, the dark web is not like Google or eBay. It is comprised of multiple discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases for viewing and purchase by different criminal actors for different fraudulent purposes.

85. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. purchasing services they would not have otherwise paid for and/or paying more for services than they otherwise would have paid, had they known the truth about Defendants' sub-standard data security practices;

b. losing the inherent value of their Personal Information;

c. losing the value of the explicit and implicit promises of data security;

d. identity theft and fraud resulting from the theft of their Personal Information;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. anxiety, emotional distress, and loss of privacy;

g. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

h. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

i. lowered credit scores resulting from credit inquiries following fraudulent activities;

j. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual

and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

k. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

86. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[49]

87. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[50]

88. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that

[49] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited March 23, 2020).

[50] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited March 23, 2020).

has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[51]

89. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendants would have no reason to tout their data security efforts to their actual and potential customers.

90. As a direct result of Defendants' failure to protect the Personal Information they were entrusted to safeguard, Plaintiffs and Class Members have been placed at an imminent and continuing increased risk of harm from identity theft and identity fraud, requiring them to spend time, money, and effort to mitigate the actual and potential impact of the Data Breach on their lives including, but limited to, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

91. Further, Defendants continue to hold Plaintiffs' and Class Members' Personal Information, and, therefore, they have an interest in ensuring that their Personal Information is secured and not subject to further theft.

CLASS ALLEGATIONS

92. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23, Plaintiffs seek certification of a nationwide class defined as follows:

[51] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited March 23, 2020).

> All persons in the United States whose Personal Information was compromised as a result of the data breach experienced by Mediant on or around April 1, 2019 (the "Class" or "Nationwide Class").

93. Pursuant to Rule 23, Plaintiff Toretto asserts claims under the law of California on behalf of a separate statewide subclass defined as follows:

> All persons in the State of California whose Personal Information was compromised as a result of the data breach experienced by Mediant on or around April 1, 2019 (the "California Subclass").

94. Pursuant to Rule 23, and in the alternative to the Nationwide Class, Plaintiff King asserts claims under the law of New Jersey on behalf of a separate statewide subclass defined as follows:

> All persons in the State of New Jersey whose Personal Information was compromised as a result of the data breach experienced by Mediant on or around April 1, 2019 (the "New Jersey Subclass").

95. Excluded from each of the above Classes are Defendants, any entity in which either Defendant has a controlling interest, and Defendants' respective officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded are all persons who make a timely election to be excluded from the Class and any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

96. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

97. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

98. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. The proposed Class includes over 200,000 individuals whose Personal Information

was compromised in the Data Breach. Class Members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

99. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The predominating common questions include:

a. Whether Defendants had a duty to protect Personal Information;

b. Whether Mediant's security measures to protect its data systems were reasonable in light of known legal requirements;

c. Whether Mediant's security measures to protect its data systems were reasonable in light of known industry standards;

d. Whether Mediant's failure to implement adequate data security measures allowed the breach of its data systems to occur;

e. Whether Donnelley's transfer of sensitive Personal Information to Mediant was reasonable in light of known legal requirements;

f. Whether Donnelley's transfer of sensitive Personal Information to Mediant was reasonable in light of known industry standards;

g. Whether Donnelley failed to adequately monitor and audit the data security systems of its vendors and business associates;

h. Whether Defendants' conduct constituted unfair or deceptive trade practices;

i. Whether Defendants' conduct was the proximate cause of the Data Breach and/or the loss of the Personal Information of Plaintiffs and Class Members;

j. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Mediant's failure to reasonably protect its data systems and data network and/or Donnelley's transfer to Plaintiffs and Class Members' Personal Information to Mediant; and,

k. Whether Plaintiffs and Class members are entitled to relief.

100. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal Information was in Mediant's possession via Donnelley at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members' damages and injuries, and Plaintiffs seek relief consistent with the relief of the Class.

101. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because they are members of the Class and are committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, and have extensive experience litigating data breach and privacy class actions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

102. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the

damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

103. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

104. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Mediant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Donnelley owed a legal duty to Plaintiffs and the Class to exercise due care in partnering with Mediant and transferring Plaintiffs' and Class Members' Personal Information to it;

c. Whether Defendants failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;

d. Whether Mediant's security measures to protect is systems were reasonable in light of known legal requirements; and,

e. Whether adherence to FTC data security recommendations, GLBA requirements, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

105. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to information regarding which individuals were affected by the Data Breach. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses)

106. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

107. Defendants collected and stored the Personal Information of Plaintiffs and Class Members for commercial gain, and promised Plaintiffs and Class Members in their privacy statements that they would keep their information safe.

108. Defendants each independently owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

109. Defendants also owed a duty of care to Plaintiffs and members of the Class to provide security of their Personal Information consistent with industry standards.

110. Defendants' duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. Defendants' duties to use reasonable care in protecting Personal Information is also required by common law, statutes and regulations such as the FTC Act and GLBA, as well as their own promises regarding privacy and data security.

111. Defendants knew, or should have known, of the risks inherent in collecting and storing Personal Information and the importance of adequate, industry-standard, and up-to-date security.

112. Mediant breached its common law, statutory, and other duties to Plaintiffs and Class Members in numerous ways, including by:

a. failing to implement security systems, protocols and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. failing to comply with industry data security standards;

c. failing to comply with statutory and regulatory Personal Information safeguards; and,

d. failing to timely disclose that Plaintiffs' and Class members' Personal Information had been improperly acquired or accessed.

113. Donnelley breached its common law, statutory, and other duties to Plaintiffs and Class Members in numerous ways, including by:

a. failing to implement security systems, protocols and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. failing to ensure that its "partners" such as Mediant had sufficient data security systems, protocols and practices before sharing sensitive information with it;

c. failing to comply with industry data security standards;

d. failing to comply with statutory and regulatory Personal Information safeguards; and,

e. failing to timely disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

114. In addition, by entering into a partnership with Mediant for the provision of proxy services, and/or holding Mediant out as its partner in providing its proxy services, Donnelley is vicariously liable for Mediant's failures as alleged herein.

115. Mediant's failure to implement proper security measures to protect the sensitive Personal Information of Plaintiffs and Class Members and Donnelley's failure to ensure Mediant had proper security measures as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act—the unauthorized access of the Personal Information of Plaintiffs and Class Members.

116. It was also foreseeable that Defendants' failure to provide timely notice of the Data Breach would result in injury to Plaintiffs and other Class Members.

117. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

118. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Class have and will suffer damages including, but not limited to: (i) the loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs

associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Mediant fails to undertake appropriate and adequate measures to protect the Personal Information of its clients' investors in its continued possession and so long as Donnelley continues to share Personal Information without ensuring the receiving party maintains reasonable and adequate security standards; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT II

NEGLIGENCE *PER SE*

(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses against Defendants)

119. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

120. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Mediant, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

121. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' Personal Information and by failing to comply with applicable industry standards. Defendants' conduct was particularly unreasonable given the sensitive nature of the Personal Information they obtained and stored.

122. Donnelley's duty to use reasonable security measures also arose under the GLBA, under which Donnelley was required to ensure companies with whom it shared Personal Information would use reasonable measures to secure it.

123. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

124. Donnelley's violation of the GLBA and its Safeguards Rule constitutes negligence *per se*.

125. Plaintiffs and Class Members are within the class of persons that the FTC Act (and similar state statutes), and the GLBA, were intended to protect.

126. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act (and similar statutes) was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class. The GLBA, with its Safeguards Rule, was similarly intended.

127. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT III

BREACH OF CONTRACT

(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses against Defendants)

128. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

129. Mediant's Privacy Policy is an agreement between Mediant and individuals who provided their personal information to Mediant, whether directly or indirectly, including Plaintiffs and Class Members.

130. Mediant's Privacy Policy states, among other things, that Personal Information "provided to Mediant by you or by third parties will be kept confidential."

131. Mediant agreed it would (a) "maintain[] physical, electronic and procedural safeguards in accordance with laws and regulations governing confidentiality and security of information"; (b) restrict "[a]ccess to personal information … to only those workers and third parties who need access to the information to perform necessary activities for Mediant"; and (c) "provide security for your information by maintaining servers that are secure and dedicated solely to the services that we provide to protect against loss, misuse, or alteration of your information."

132. Mediant's Privacy Policy further states: "by holding a position in, or otherwise being materially connected with, an organization that has appointed us to perform services on your behalf you consent to Mediant's collection, use and disclosure of your personal information as described in this Privacy Statement. Consent can be express or implied. Express consent can be verbal or written. For example, you may have expressly provided consent for the third party to share information with us when you completed an application for brokerage services. Or it may be concluded that you provided implied consent by an action you have taken or not taken, or where the context reasonably requires that we have and use information to carry out what you have asked us to do, such as when you process a transaction on a Mediant or Mediant-hosted web site."

133. Plaintiffs and Class Members formed a contract with Mediant when they provided Personal Information to Mediant, whether directly or indirectly, subject to the Privacy Policy.

134. Mediant breached its agreement with Plaintiffs and Class Members by failing to protect their Personal Information, including failing to comply with the promises and obligations set forth in the Privacy Policy.

135. As a direct and proximate result of Mediant's breach, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein.

136. Donnelley's Privacy Notice is an agreement between Donnelley and individuals who provided their personal information to Donnelley, whether directly or indirectly, including Plaintiffs and Class Members.

137. Donnelley's Privacy Notice states, among other things, that "[t]he security of your personal information is important to us," and agreed to (a) "use reasonable physical, electronic and procedural safeguards to protect the personal information [it] collect[s]," (b) "use[] reasonable measures to safeguard personally identifiable information from loss, theft, misuse, alteration and unauthorized access or destruction, and (c) to "maintain appropriate physical, electronic, and procedural safeguards to protect your personal data."

138. Plaintiffs and Class Members formed a contract with Donnelley when they provided Personal Information to Donnelley, whether directly or indirectly, subject to the Privacy Notice.

139. Donnelley breached its agreement with Plaintiffs and Class Members by failing to protect their Personal Information by sharing it with Mediant without ensuring Mediant had adequate data security to protect it, in breach of the promises and obligations set forth in the Privacy Notice.

140. As a direct and proximate result of Donnelley's breach, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein.

COUNT IV

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses against Defendants)

141. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein, and assert this claim in the alternative to their breach of contract claims to the extent necessary.

142. Plaintiffs and Class Members directly and indirectly provided their Personal Information to Defendants in order to purchase securities.

143. As part of these transactions, Defendants agreed to safeguard and protect the Personal Information of Plaintiffs and Class Members. Implicit in the agreements between Defendants and Class Members was the obligation that Defendants would use the Personal Information for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

144. Additionally, Defendants implicitly promised to retain this Personal Information only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the Personal Information of Plaintiffs and Class Members from unauthorized disclosure or access, and to use reasonable care in transferring that information to third parties.

145. Plaintiffs and Class Members entered into implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with industry standards.

146. Plaintiffs and Class Members would not have directly or indirectly provided and entrusted their Personal Information to Defendants in the absence of the implied contracts with Defendants. The safeguarding of Plaintiffs' and Class Members' Personal Information was critical to realize the intent of the parties.

147. Defendants breached their implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' Personal Information, which was compromised as a result of the Data Breach.

148. Defendants' acts and omissions have materially affected the intended purpose of the implied contracts.

149. As a direct and proximate result of Defendants' breaches, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein.

COUNT V

BREACH OF CONTRACTS OF WHICH PLAINTIFFS ARE THIRD PARTY BENEFICIARIES

(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses against Defendants)

150. Donnelley entered into contracts with public companies and mutual funds to provide and perform proxy services. In some instances, Mediant also directly contracted with public companies and mutual funds to provide and perform proxy services.

151. On information and belief, each of those respective contracts contained provisions requiring Donnelley and/or Mediant to protect the personal information of the investor information that Donnelley and/or Mediant received in order to provide such proxy services.

152. On information and belief, these provisions requiring Donnelley and/or Mediant to protect the personal information of the company/mutual fund's investors was intentionally included for the direct benefit of Plaintiffs and Class Members, such that Plaintiffs and Class Members are intended third party beneficiaries of these contracts, and therefore are entitled to enforce them.

153. Defendants breached these contracts by not protecting Plaintiffs' and Class Members' Personal Information, as stated herein.

154. As a direct and proximate result of Defendants' breaches, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein.

COUNT VI

UNJUST ENRICHMENT

(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses against Defendants)

155. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein, and assert this claim in the alternative to their breach of contract claims to the extent necessary.

156. Plaintiffs and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Defendants and which was ultimately stolen in the Data Breach.

157. Defendants were benefitted by the conferral upon them of the Personal Information pertaining to Plaintiffs and Class members and by their ability to retain and use that information.

158. Defendants appreciated and had knowledge of the benefits conferred upon them by Plaintiffs and Class Members. For example, Donnelley stated in its Privacy Notice that: (1) it uses, stores and processes the personal information it collects to provide users with information, products and services which they request or similar products or services; (2) the information is also used to improve Donnelley's existing services and the content of its site; (3) Donnelley also shares personal information it collects with its affiliates, business partners, service providers, subsidiaries, vendors, consultants and other service providers to perform work on its behalf; and (4) the information may also be shared with third parties to offer or provide related services. Likewise, Mediant states in its Privacy Policy that it uses personal information it collects for marketing purposes.

159. Defendants also understood and appreciated that the Personal Information pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that Personal Information.

160. But for Defendants' willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted with

Defendants. Further, if Defendants had disclosed that their data security measures were inadequate, they would not have been permitted to continue in operation by regulators, their clients, and participants in the marketplace.

161. As a result of Defendants' wrongful conduct as alleged herein, Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members. Among other things, Defendants continue to benefit and profit from using Personal Information in the regular course of their businesses while its value to Plaintiffs and Class Members has been diminished.

162. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

163. Under the common law doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiffs and Class Members in an unfair and unconscionable manner. Defendants' retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

164. The benefit conferred upon, received, and enjoyed by Defendants was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain the benefit.

165. Defendants are therefore liable to Plaintiffs and Class Members for restitution in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically the value to Defendants of the Personal Information that was stolen in the Data Breach

and the profits Defendants are receiving from the use of that information in the course of their businesses.

COUNT VII

DECLARATORY JUDGMENT

(On Behalf of Plaintiffs and the Nationwide Class against Defendants)

166. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

167. Defendants, who each promised in their privacy statements to protect Plaintiffs' and Class Members' Personal Information, still possess the now-compromised Personal Information.

168. Mediant has only superficially represented to Plaintiffs and the Class that it has made unspecified "updates" remedying the security issues that allowed hackers to obtain Plaintiffs' and Class Members' unencrypted Personal Information via Mediant's business email accounts. Mediant has provided no assurances that Plaintiffs' and Class Members' information is actually safe, or that it has been deleted from Mediant's systems if it is no longer needed. Likewise, Donnelley has provided no assurances that it has remedied its procedures for ensuring third parties with whom it shares sensitive personal information have adequate security measures to keep it safe.

169. Accordingly, Defendants have not satisfied their obligations and legal duties to Plaintiffs and the Class. In fact, now that Defendants' lax approach towards data security has become public, the information in their possession is more vulnerable than it was prior to announcement of the Data Breach.

170. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the state and federal statutes described in this Complaint.

171. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Personal Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Personal Information. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injuries as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

172. Pursuant to the Declaratory Judgment Act, Plaintiffs seek a declaration that: (a) Defendants' existing data security measures do not comply with their obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Donnelley must have policies and procedures in place to ensure third parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(h), *infra*, and must comply with those policies and procedures; (2) Mediant must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiffs' and Class Members' Personal Information if it is no longer needed in order to prevent further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Mediant's systems on a periodic basis, and ordering Mediant to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. encrypting Personal Information and segmenting Personal Information by, among other things, creating firewalls and access controls so that if one area of Mediant's systems is compromised, hackers cannot gain access to other portions of Mediant's systems;

e. purging, deleting, and destroying in a reasonable secure manner Personal Information not necessary for its provisions of services;

f. conducting regular database scanning and security checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Mediant customers must take to protect themselves.

COUNT VIII

VIOLATION OF CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq.*
(On Behalf of Plaintiff Toretto and the California Subclass against Defendants)

173. Plaintiff Toretto restates and re-alleges the preceding paragraphs as if fully set forth herein.

174. Plaintiff Toretto and California Subclass Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Defendants and which was ultimately stolen in the Data Breach.

175. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

176. Defendants are each a business that owns, maintains, and licenses Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff Toretto and California Subclass Members.

177. By failing to implement and maintain reasonable security procedures and practices appropriate to protect Plaintiff Toretto's and California Subclass Members' Personal Information from unauthorized access, use, and disclosure, Defendants each violated Cal. Civ. Code § 1798.81.5.

178. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must describe "what happened" and include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

179. Defendants are each a business that owns or licenses computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

180. Plaintiff Toretto and California Subclass Members' Personal Information includes Personal Information as covered by Cal. Civ. Code § 1798.82.

181. Because Defendants reasonably believed that Plaintiff Toretto's and California Subclass Members' Personal Information was acquired by unauthorized persons during the Data Breach, Defendants each had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

182. By failing to disclose the Data Breach in a timely and accurate manner, Defendants each violated Cal. Civ. Code § 1798.82.

183. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff Toretto and California Subclass Members suffered damages, as described above.

184. Plaintiff Toretto and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT IX

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiff Toretto and the California Subclass against Defendants)

185. Plaintiff Toretto restates and re-alleges the preceding paragraphs as if fully set forth herein.

186. Defendants are each a "person" as defined by Cal. Bus. & Prof. Code § 17201.

187. Defendants violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

188. Defendants' "unfair" acts and practices include:

a. Mediant failed to implement and maintain reasonable security measures to protect Plaintiff Toretto's and California Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Mediant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. Likewise, Donnelley failed to identify Mediant's foreseeable security risks and ensure they had been remedied prior to partnering with Mediant and sharing Plaintiff Toretto's and California Subclass Members' Personal Information with it. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff Toretto and the California Subclass, whose Personal Information has been compromised.

b. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' information and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, GLBA, 15 U.S.C. § 6801(b), and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Defendants' failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendants' inadequate security, affected individuals could not have reasonably avoided the harms that Defendants caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code §§ 1770(a)(5), 1798.81.5, 1798.82, 15 U.S.C. § 45, and 15 U.S.C. § 6801(b),

189. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification); California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA"), in particular, the CLRA's proscription against misrepresenting the characteristics or qualities of services, § 1770(a)(5); the FTC Act, 15 U.S.C. § 45; the GLBA, 15 U.S.C. § 6801(b) (as to Donnelley); and California common law.

190. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Toretto and California Subclass Members' Personal Information, including ensuring that third-parties with whom Personal Information was shared implement and maintain such measures, which were direct and proximate causes of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Toretto and California Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801(b) as to Donnelley, and California's Customer Records Act, Cal.

Civ. Code §§ 1798.80, *et seq*., which were direct and proximate causes of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Toretto's and California Subclass Members' Personal Information; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Toretto's and California Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801(b) as to Donnelley, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.

191. Defendants' omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

192. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff Toretto and California Subclass Members were injured and lost money or property, the premiums and/or price received by Defendants for their goods and services, the loss in value of their Personal Information; loss of the benefit of their bargains with Defendants in that Defendants agreed to protect their Personal Information and failed to do so and the value of their Personal Information was lost as a result; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing payment cards;

loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

193. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff Toretto's and California Subclass Members' rights. Defendants' acknowledgement of numerous breaches within the financial industry put them on notice that their security and privacy protections were inadequate.

194. Plaintiff Toretto and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT X

VIOLATION OF NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law §§ 349, *et seq.*
(On Behalf of the Nationwide Class against Mediant)

195. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

196. Mediant is headquartered in this District and engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures

in the face of known cyber security threats, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that Mediant did not reasonably or adequately secure Plaintiffs' and Class Members' Personal Information; and

e. Omitting, suppressing, and concealing the material fact that Mediant did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

197. Mediant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Personal Information.

198. Mediant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs' and Class Members' rights. Past data breaches and breaches within the financial services industry put Mediant on notice that its security and privacy protections were inadequate.

199. As a direct and proximate result of Mediant's deceptive and unlawful acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing payment cards; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

200. Mediant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the more than 200,000 individuals affected by the Data Breach.

201. The above deceptive and unlawful practices and acts by Mediant caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid.

202. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

A. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs as the class representatives and the undersigned counsel as class counsel;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Personal Information;

C. For equitable relief compelling Defendants to use industry-standard security methods and policies with respect to data collection, storage and protection, and sharing of

information, and to dispose of Plaintiffs' and Class Members' Personal information in their possession as soon as it is no longer needed;

D. For an award of damages, including nominal and statutory damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: March 30, 2020

/s/ *Amanda Peterson*
Amanda Peterson (Bar No. AP1797).
MORGAN & MORGAN
90 Broad Street, Suite 1011
New York, NY 10004
Telephone: (212) 564-4568
apeterson@forthepeople.com

Norman E. Siegel (*pro hac vice* forthcoming)
J. Austin Moore (*pro hac vice* forthcoming)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com

Patricia N. Syverson (*pro hac vice* forthcoming)
BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
600 W. Broadway, Suite 900
San Diego, California 92101
Telephone: (602) 274-1100
psyverson@bffb.com

Elaine A. Ryan (*pro hac vice* forthcoming)
Carrie A. Laliberte (*pro hac vice* forthcoming)

BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
2325 E. Camelback Road, #300
Phoenix, Arizona 85016
Telephone: (602) 274-1100
eryan@bffb.com
claliberte@bffb.com

Counsel for Plaintiff and the Class